Towards a Pervasive Access Control within Video Surveillance Systems

Dana Al Kukhun, Dana Codreanu, Ana-Maria Manzat, Florence Sèdes

Towards a Pervasive Access Control within Video Surveillance Systems

Dana Al Kukhun[1], Dana Codreanu[2], Ana-Maria Manzat[2], and Florence Sedes[2]

[1] Faculty of Computer Informatics, Amman Arab University
Amman - Jordan
danakukhun@gmail.com
[2] Universite de Toulouse – IRIT – UMR 5505,
31062 Toulouse, France
{Firstname.lastname}@irit.fr

Abstract. This paper addresses two emerging challenges that multimedia distributed systems have to deal with: the user's constant mobility and the information's sensitivity. The systems have to adapt, in real time, to the user's context and situation in order to provide him with relevant results without breaking the security and privacy policies. Distributed multimedia systems, such as the one proposed by the LINDO project, do not generally consider both issues. In this paper, we apply an access control layer on top of the LINDO architecture that takes into consideration the user's context and situation and recommends alternative resources to the user when he is facing an important situation. The proposed solution was implemented and tested in a video surveillance use case.

1 Introduction

With the proliferation of multimedia data and applications in a distributed and dynamic environment, many solutions for indexing and accessing multimedia collections are proposed to cope with emerging challenges like: distributed storage and decentralized processing, choice of the indexing algorithms, real time and location-aware information retrieval, optimization of resources consumption (e.g., CPU, RAM, storage, network communications).

In the multimedia contents' management another important issue is raised by the user's mobility and the fact that he/she wants and needs to access the contents from anywhere at any moment: the system's and contents' security. This issue concerns five criteria:

- *Confidentiality*: assurance that the information is shared only among authorized persons or organization;
- *Privacy*: assurance that the identifiable data relating to a person is protected during the information exchange/sharing;
- *Integrity*: assurance that information is authentic and complete;
- *Availability*: assurance that the information is accessible when needed, by those who need it;
- *Traceability*: ability to verify the history, location, or application of an item.

In this highly dynamic context, the multimedia database systems security becomes a critical issue. Many application domains (e.g., medical, military, video surveillance) may contain sensitive information which should not be or could only partially be accessed by general users. Therefore, it is essential to support security management of multimedia systems and design security models accordingly.

On top of that, we have to consider also that the users are more and more mobile and they need to access the system from anywhere, in real time. There are some cases when the user's context and situation are important, and in order to accomplish a certain task the user must have access to the information. A definition of system security is provided by [1]: "a computing system is secure, if and only if it satisfies the intended purposes without violating relevant informational (or other) rights". Thus, a solution to this privacy and security problem has to be found in order to provide the user with some contents without breaking the system's security.

In this paper, we present a new access control layer on top of the distributed architecture proposed by the LINDO project[1], which considers the user's context and situation within the privacy and security management process. The project's objective was to build a distributed system for multimedia content management, and to ensure effective indexing and storage of data acquired in real time, while considering the resource consumption optimization. The project did not address the issues linked to data privacy and security. The users have full access to all contents after an authentication.

Our objective is to include, within the LINDO framework, the access control in order to attain a pervasive accessibility that enables the user to access multimedia contents at anytime, from anywhere, without breaking the system's security.

In the next section we introduce a state of the art covering distributed access control management, and multimedia access control. The LINDO approach is described in section 3. In section 4, we apply an access control layer on top of the LINDO architecture. In section 5, the adaptive access control solution is illustrated through a video surveillance use case. Finally, conclusions and future work directions are provided in section 6.

2 Related Work

In order to deal with the challenges raised by the big multimedia collections, more and more systems use a distributed architecture for their management. An advantage of this kind of systems is that they benefit from the distributed storage and processing of the contents and the obtained metadata, and thus, a better performance. However, a major problem that these systems encounter is the heterogeneity of indexing algorithms and of the generated metadata and the control of user's access to the system.

In some of the studied systems, complete access is granted after successful authentication of the user. In most application domains a more sophisticated and complex access control is required. In the next section we detail different strategies for distributed access control.

[1] http://lindo-itea.eu/

2.1 Distributed Access Control

In order to guarantee full protection of the confidential information within a decentralized system, accessibility should be controlled through all the communication channels: the application level, the middleware level, the operating system level and finally through the network.

Many models were defined over the years to address the access control issue, without necessarily considering the contents distribution and the user's mobility: DAC [2], MAC [3], RBAC [4], and XACML [5].

In pervasive systems, an important issue that has to be taken into account in the access control management is the user's context and situation in the moment when he/she is accessing the system. More precisely, the system has to react, in real time, to the constant change in the user's context and situation, in order to provide an adaptive access according to the user's needs.

2.2 Context-Aware Access Control

In ubiquitous computing environments, users are mobile and typically accessing resources using mobile devices. As a result, the user's context (e.g., time, location, network connection, device) becomes highly dynamic, and thus, granting him access to the contents without taking his current context into account can compromise the system's security as the user's access privileges do not only depend on "Who the user is", but also on "Where the user is" and "What is the user's state and the state of the user's environment". Thus, access control in ubiquitous applications requires that the user's privileges dynamically change based on his context and role. Thus, permissions assignment for a user has become more complex and dependent on his context.

Many research works have proposed to extend the RBAC model in order to take into account the context's evolution:

- Temporal RBAC [6] considers time as a constraint for the activation and deactivation of a role.
- Spatial RBAC [7] incorporates location information associated with roles in order to permit location-based security policies. Permissions are dynamically assigned to the role dependent on location.
- Dynamic Role Based Access Control [8] dynamically adjusts role and permission assignments based on context information.
- UbiquiTous Role-Based Access Control [9] considers the time and the location of the user as important elements for the activation and disabling of a role. Each role has a state which is changeable during a session.
- [10] provides a context-aware RBAC model that separates context management from the access control model in order to facilitate decision-making in cases where an authorization decision is connected to several contextual constraints.

All these models tie permission assignment to the user's identity and role but also to his contextual attributes, but they are not flexible and responsive enough to deal with any type of situation confronting the user (emergency, un-expected event, etc.).

2.3 Situation-Aware Access Control

The need of situation-awareness in access control was first expressed by [11], who highlighted the importance of providing a security scheme that would relax access rules in order to enable users to meet exceptional circumstances (disasters, medical emergencies or time-critical events).

The works of [12] have also highlighted the importance of providing a flexible security system that would offer more than yes or no answers and that would not rely on predefined solutions in meeting unanticipated access demands.

A flexible solution, called "Break-Glass", was adopted as a standard within health care systems [13]. The solution helps users to confront emergent situations by granting them access to unauthorized needed resources. Despite all the protective steps accompanying it, the "Break-Glass" is an extreme solution that enables users to perform illegitimate intrusions and unjustified access attempts. Therefore, various research works have focused on either controlling the usage of "Break-Glass" by improving its modeling and on facilitating it's integration within the conventional access control models in order to confront the privacy and integrity threats or on proposing other less risky situation-aware access control solutions: [14], [15].

The flexibility level offered by these access control models is directly proportional to the risk of violating the system's security. The more the access control flexibility is performed on a rule-based, predefined or assisted manner, the less the violation risks are introduced. The more the flexibility is provided in an automatic and ad hoc manner, the more the risk level is elevated.

When applying these access control models to the multimedia domain, the things become more complex, especially if a fine-grain access control is needed.

2.4 Multimedia Access Control

Many solutions have been proposed in order to secure the access to multimedia databases and systems. While some authors were interested in the security of the connection to the systems and of the distribution of the contents [16], others were focused on the content-based multimedia access control with fine-grain restrictions at a specific level of the multimedia data [17].

[18] proposes a framework that addresses multi-level multimedia access control by adopting RBAC, XML and Object-Relational Databases. The authors associated roles to users, IP addresses, objects and time periods. All multimedia contents handled by their system have to be segmented. Only the objects which have roles associated to are extracted from the multimedia contents.

[19] studied the confidentiality and privacy issues in the context of a video surveillance system. They defined access rights to different hierarchical objects that can be extracted from the video contents. They focused on the detection of suspicious events.

The management of access control in pervasive environments has evolved over the last years and it takes into account the user's context in the moment when he is interacting with the system. Meanwhile, the distributed multimedia systems do not concentrate their effort on these issues, they consider the management of the contents and their indexing, without the intention of providing solutions for the optimization of the resource consumption.

In order to offer a better response to the user's needs, a system has to leverage between the resource consumption, the returned results and the security. The LINDO project, detailed in the next section, offers a solution for optimal resource consumption, but it does not treat the much attention to the access control.

3 Distributed Multimedia Approach Proposed within LINDO Project

The main goal of the LINDO project (Large scale distributed INDexation of multimedia Objects) is to define a distributed system for multimedia content management, while focusing on the efficient use of the resources in the indexing and query processes. Thus, not only the multimedia contents storage is distributed, but also the indexing process. The originality of this solution is that:

- the content is not moved to indexing servers, but the indexing algorithms are deployed on the remote servers where the content is acquired;
- the indexing process is accomplished in two steps: at acquisition and at query time.

A more detailed presentation of the LINDO architecture can be found in [20].

In order to reduce the resources consumption, the architecture allows the indexing of multimedia contents to be accomplished at acquisition time (i.e., implicit indexing) with some algorithms which extract generic features from the content (e.g., person detection, dominant color detection) and on demand (i.e., explicit indexing) with some algorithms which extract more detailed features (e.g., person recognition, registration plate detection). This avoids executing all the indexing algorithms at once and producing metadata that might never be used, but raises access rights issues concerning the explicit indexing.

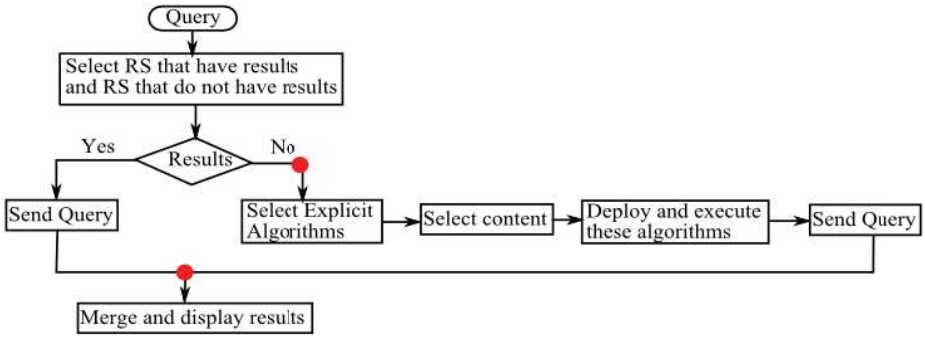

Fig. 1. Query Processing Flow Chart

The query processing (Figure 1) begins with the query specification. First, the query is executed on the metadata collection on the central server, in order to select the remote servers that could provide answers to the query and it is sent for execution to the selected servers. Among the servers that were not selected at the first step, there

could be some servers that contain relevant information that has not been indexed with the right algorithms. For this reason, supplementary algorithms are selected and executed on a sub-collection of multimedia contents. All the results obtained from the remote servers are sent to the central server, where they are combined and displayed to the user.

In this system, the user has full access to all the functionalities and resources after an authentification process. The pervasive access to the system emphasizes the access control and security issues, because of multimedia contents sensitivity and privacy protection laws that impose anonymity constraints. These issues were not treated in the LINDO project.

4 Adding an Access Control Layer to the LINDO Architecture

When applying one of the solutions presented in section 2 to the LINDO system, the lack of results returned to a user's query might not only be due to the lack of results existing within the system but also due to access restrictions imposed by the security layer. This lack of results could be a problem for the user, and prevent him from realizing his task. In order to surpass this limitation, we propose to add an access layer that customizes user's access and is responsible for managing:

The access rights granted to users or services demanding access to multimedia contents that vary according to their role, their context and their situation.

The access rights for executing queries that employ the explicit indexing algorithms: the risk of disclosing personal or confidential information arises with the level of detail sought and provided by the indexing algorithm. For that we have introduced two "checking points" (illustrated in Figure 1, before executing explicit indexing algorithms and before displaying the results) where the user's access rights in his given situation are verified.

In order to achieve these goals, we employ PSQRS (Pervasive Situation-aware Query Rewriting System), an adaptive decision-making system that confronts access denials taking place in real-time situations by rewriting access requests in order to offer alternative-based access solutions, presented in section 4.2. This approach is based on the RBAC model and the XACML standard, and it exploits the user's context (e.g., location, time) and his situation (i.e., the emergency level of the task the user is solving when accessing the system).

The access control relaxation that we propose to carry out respects the access rights defined to protect the multimedia content and applies the adaptive decision-making at two functionalities:

- The explicit indexation execution and the indexing algorithms selection.
- The multimedia contents filtering and presentation.

More precisely, in the two red points illustrated in Figure 1, a matching function is executed, in order to establish based on user's profile and situation if he has the right to run explicit algorithms, respectively to access the content:

$$\Gamma.:(\text{Up, Situation, Policy}) \rightarrow \text{Permit/Deny},$$

where Up is the user's profile, the Situation is a level of emergency (explicitly provided by the user, or inferred from his location, context and other explicit information provided by the user) and Policy is the set of rules that define the security policy of the system.

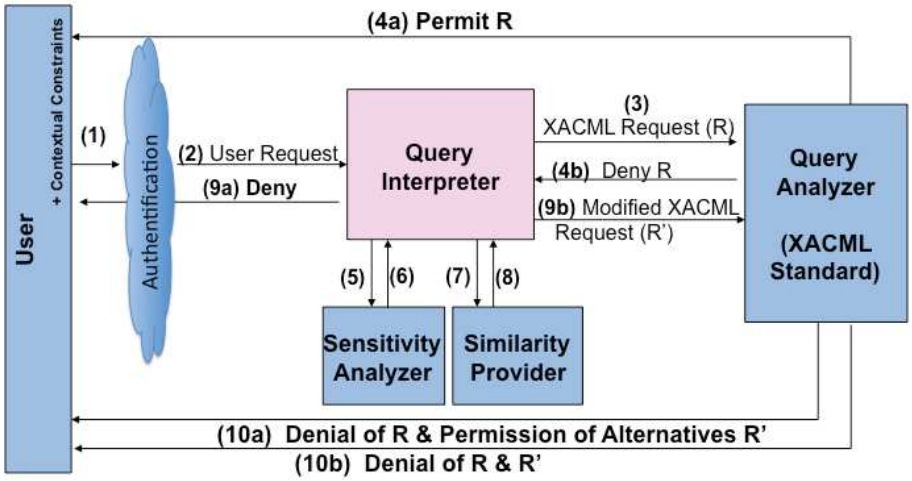

Fig. 2. The PSQRS Architecture

The user profile is defined as:

$$Up = < Uid;Name;Login;Password;RoleId >$$

where Uid is the user's id, Name is the user's name, Login is the user's login, Password is the user's password and RoleId represents the role that is associated to this user for the current access to the system.

An access rule is defined as:

$$Rule = < RuleId;RoleId;Action;Context;Permission >$$

A rule defines a certain Permission (Permit or Deny) for a certain role (i.e, RoleID) and Action (e.g., explicit indexing, object visualization) in a certain Context.

Next, we introduce the detailed functionality of the PSQRS architecture.

4.1 The PSQRS Architecture

As illustrated in Figure 2, the PSQRS architecture contains several components and the sequence of its functionality starts from the user, who enters the system through an authentication portal (step 1) and launches an access request to a certain element (step 2). This request will be interpreted by our Query Interpreter that will translate the request into an XACML request and send it to the Query Analyzer (step3). The request (R) will be analyzed in consideration with the user's profile – automatically extracted at the sign in process -and according to his context. As the analysis finishes,

the Query Analyzer would send the result directly to the user if it's a Permit (step 4a) or back to the Query Interpreter, if it's a deny (step 4b).

In a deny situation the adaptive situation-aware query rewriting mechanism will take place as follows: the Query Interpreter will check the sensitivity of the situation with the help of the Sensitivity Analyzer (steps 5, 6) and according to the situation's importance level, the Query Interpreter will search for similar or alternative resources through the Similarity Provider (steps 7, 8) and employ them to rewrite the XACML request (R') and send it again to the Query Analyzer that will analyze the request and transfer the result back to the user (steps 10a,10b).

4.2 The Fusion of PSQRS and LINDO System

In order to include this access control layer to the LINDO system, some changes have to be done into the system. More precisely, from a functional point of view, each time an access to the system is demanded (the red circles in Figure 1), the PSQRS system is used before applying the explicit indexation and before displaying the results. From an architectural point of view, the system's architecture, detailed in [1], was enhanced with several modules and functionalities.

Thus, in Figure 3, the modules that were added or modified are displayed in red. Almost all the changes are encountered on the central server:

- the Authentification Module was added. This module determines if the user is known by the system and retrieves his profile based on his context. Each user request passes through this module, thus if between two requests the user's context changes his profile could change also.
- the Access Control Module was added. In this module were included the Query Interpreter, the Sensitivity Analyzer and the Similarity provider. All information that is sent to the user passes through this module in order to apply a possible access control adaptation.
- the Terminal Interface was modified in order to capture the user's context and situation.
- a database with RBAC roles, rules and users' profiles was included into the Metadata Engine. It contains also information on the access adaptation.
- the Query Analyzer was integrated into the Request Processor.
- on the Remote Server, only the Access Manager was modified. In fact, a new functionality was added to this module: the execution of an indexing algorithm.

For each identified RBAC role, access rights to the multimedia contents, the explicit indexing and the execution of certain indexing algorithms are specified according to the context the user can have when accessing the system. The user's situation is captured by the system in an implicit (by analyzing the context) or explicit way (in the user interface). In order to offer alternatives to the user according to his situation, the Similarity Provider can select other multimedia contents or execute some algorithms that extract information from the content or modify it in order to respect the user's access rights.

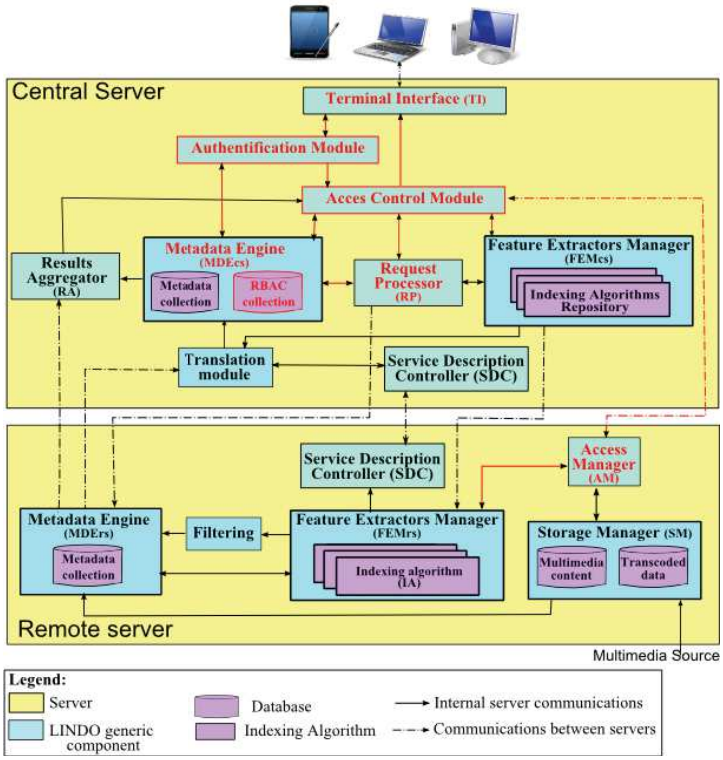

Fig. 3. The modified LINDO Architecture which incorporates the PSQRS approach

In the next section, we present a video surveillance use case, where the implementation of our proposal is used to overcome the lack of answers. As we will illustrate, the system will modify the query processing and will adapt access decisions according to the level of importance of the querying situation.

Table 1. Examples of access rights

Role	**User's Context**	**Content**	**Action**	
			See passenger's faces	**Explicit Indexation**
Security agent	Control room	All	Allow	Allow
	Stations	From metro cameras	Deny	Allow, only object tracking
		From bus cameras	Deny	Deny
Policeman	Control room	All	Allow	Allow
	Stations	From metro cameras	Allow	Allow, only object and person tracking
		From bus cameras	Allow	Deny

5 The Video Surveillance Use Case

This use case concerns a public transportation company that placed surveillance cameras in buses and metros, around the stations and ticket machines.

This system is used by the security agents and police officers. Thus we can identify two roles: security agent and policeman. The access to the system can be done from the control room, or from the stations using a mobile phone. For each role a set of restrictions can be established, based on the existing laws and on the tasks that they have to deal with. Table 1 provides some examples of the access rights given to each role, in a certain context and for a certain multimedia content. For example, a security agent does not have the right to see passenger's faces nor to execute the explicit indexation when he is not in the control room, and he wants to access the multimedia content acquired by the video cameras located in buses.

In this use case we can identify several situations: the security agent investigates on a lost object incident, a lost child research, a bomb attach. Each one of these situations has attached a level of importance (Level=0 is a normal situation, Level=5 is the most important situation).

Let us consider the following scenario: *Taking the bus 2 from "Trocadero" station to "Place d'Italie" station at 14:15, Helen has forgotten her red bag in the bus. As soon as she realized, she went out to report the problem at the information counter in a metro station.*

A typical treatment of such situations goes through the customer service agent who opens a lost object incident with the identification number 1234, takes the descriptions and transmits them to the security agent on site. The security agent will follow different steps in order to find the object. He will check if the object has already been found or returned to the lost and found office by someone. Otherwise, he will execute a query on from his mobile device to check if the object is still in the same location or if somebody took it.

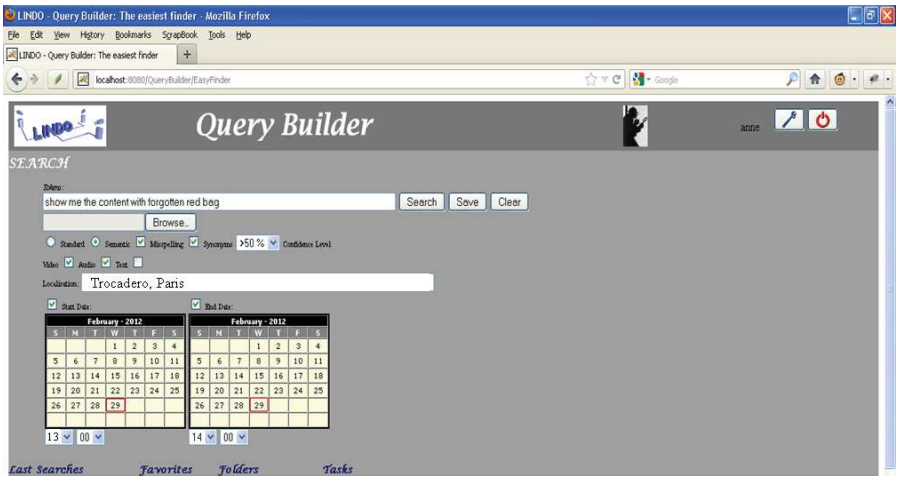

Fig. 4. LINDO user interface

The agent will formulate the following query, in the terminal interface presented in Figure 4 : Find all videos containing a red bag, forgotten in bus nr 2 at Place d'Italie, Paris station, on the 1st of December, between 2:00pm and now (3:00pm), related to the incident number 1234.

In the next sub-sections we present the application of two strategies for ensuring the access control: taking in to account only the user's context, and considering also his situation.

5.1 Applying a Context Access-Control Strategy

The query is processed and translated into XQuery. This query transformation is detailed in [20].

The query processing begins by locating the servers responsible for managing the data captured by the cameras located in the bus nr 2, which passed between 14h00 and 15h00 at Place d'Italie station. Next, a filtering step is performed to restrict the search within the segments captured between 14:00 and 15:00.

The system will then, determine a list of indexing algorithms that would meet the needs and context expressed within the query. Supposing that all the selected algorithms were executed during the implicit indexation process, the query will be executed and thus the video segments that contain red objects are retrieved.

A filtering process is applied to take into account access control rules. Analyzing the access rights assigned to the security agent, we find that he is not authorized to access the videos containing passenger's faces when he is not in the control room. Therefore, considering these access restrictions, the system will eliminate the segments that contain person faces and finally return to the user the list of segments that contain a red object (if available).

5.2 Applying a Situation Access-Control Strategy

The search results returned to the security agent in this case might be insufficient. The red bag might be present in the unauthorized segments containing passenger faces.

An adaptive solution can be employed when the system identifies access challenges related to the user's context or at an important situation. In this scenario, the "lost object" situation is explicitly provided by the agent through the incident number.

The implementation of the adaptive solutions is performed by the PSQRS that adapts decision-making by rewriting the XACML queries.

As shown in Table 2, the richness of the elements that we can embed within an XACML query enables it to describe the contextual attributes characterizing:

- the requested content in the "resource" tag, in red in the figure,
- the user launching the request in the "subject" tag, in bold in the figure
- the situation at which the user has launched the access request in the "environment" tag, in blue in the figure.

The importance level of the situation will determine the level of adaptation.

As the adaptive querying mode is triggered, the query processing mechanism will change to ensure the success of the search by providing a variety of adaptive solutions in correspondence with the situation's sensitivity level.

The adaptation process in this scenario will follow another scheme since the lost object situation is judged to be of higher importance (Level=1). Hence, the Similarity Provider component will be replaced by an Adaptive Solutions Provider. This component will provide some predefined solutions that could bypass the access control challenge or would assist the user in adapting and reformulating his query by pointing out the access challenge and offering him adaptive solutions that would suit his context, the solutions are often saved in a predefined database. Table 3 shows examples of the solutions that the system can offer.

Table 2. XACML request embedding the user's query

```
<Request>
    <Subject>
        <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:subject:subject-id">
            <AttributeValue>John Smith</AttributeValue> </Attribute>
        <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
            <AttributeValue>Security Agent</AttributeValue> </Attribute>
        <AttributeAttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:securityAgent-id">
            <AttributeValue>sa2023</AttributeValue></Attribute>
    </Subject>
    <Resource>
        <ResourceContent>
            <UserQuery>  <QueryInText> Find all videos containing a red bag, forgotten in
bus nr 2 at Place d'Italie station, Paris, on the 1st of December, between 2:00pm and now
(3:00pm)</QueryInText>
                <MediaLocation> bus nr 2 at Place d'Italie station, Paris </MediaLocation>
                <MediaFormat>Video</MediaFormat>
                    <TimeSpan>
                        <From>2012-12-01T14:00:00</From>
                        <To> 2012-12-01T15:00:00</To>
                    </TimeSpan>  </UserQuery>
        </ResourceContent>
    </Resource>
    <Action>
        <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:action:action-id">
            <AttributeValue>Read</AttributeValue> </Attribute>
    </Action>
    <Environment>
        <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:environment:environment-id">
            <AttributeValue>Situation</AttributeValue> </Attribute>
        <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:environment:situation-id">
            <AttributeValue>Forgotten Object</AttributeValue> </Attribute>
        <Attribute AttributeId="urn:oasis:names:tc:xacml:2.0:environment:sitLevel-id">
            <AttributeValue>1</AttributeValue>
         </Attribute>
    </Environment>
</Request>
```

New solutions can also be inserted to the adaptive solutions database through a learning mechanism that detects the solutions that users employ when encountered with access challenges in real time.

The success of the adaptive solutions suggested by the users would eventually be more efficient if they knew the reason behind the access denial. The error messages that often accompany the returned access denial results can serve as indicators to help the users in finding alternative solutions.

Therefore, the adaptive solution for this example will modify the treatment process and will: neglect the filtering step responsible for imposing the access control constraints and replace it with an adaptive step-related to the presentation of resources with unauthorized content.

Table 3. The solutions that our adaptive query processing module can use

Problem	**The adaptive solution**
The privacy law imposing the protection of anonymity of audiovisual contents.	
Passenger faces are not authorized	Display the content after the execution of an algorithm that applies a blur face function.
Voices are not-authorized	Use an algorithm for speech-to-text transcription.
Video volume	
Lack of storage capacity on the user's machine	Use a compression algorithm in order to obtain a smaller file.
Format not supported by the user's machine	Use a conversion algorithm into a compatible format
Download problems due to a low bandwidth	Use a summarization algorithm in order to obtain a concise version of the content.

By applying this process to the scenario described above, the system will return the video segments taken from the Trocadero station between 14:00 and 15:00 and containing a red object. These results will be filtered in order to detect the unauthorized segments (containing passenger faces). This is where the system will apply the adaptation process that would filter the display to conform with the access restrictions imposed by the system.

The adaptation will be performed through a face detection step and the use of an algorithm that applies a "blur function" to protect the privacy of passengers appearing in these segments in order to return to the user a list of relevant results that respect the access rules.

6 Conclusions

In this paper, we have presented an adaptive approach for access control management within multimedia distributed systems, by considering the user's context and situation. Our solution overcomes the access denials that take place in real time access demands by modifying the query processing mechanism and by providing adaptive solutions to bypass the access control constraints. The proposed solution has been validated within the LINDO framework in the context of a video surveillance use case. We applied and validated the same access control approach for other use cases, such as Health care Systems [21].

The adaptive and alternative based situation-aware solution can increase the complexity of processing the request, but if we consider the usefulness of the results

provided in real time and the fact they do not violate the access rights defined by the privacy law, this complexity seems quite acceptable.

In future works, we aim to extend our proposal by taking into account different contextual elements that might also influence the accessibility to multimedia content (e.g., hardware, network bandwidth, etc.) and to apply the adaptive process not only at the presentation level but also at the choice of the explicit indexing algorithms that are protected by RBAC constraints. We plan to exploit users profiles and behavior in order to automatically determine the alternative solutions to use in case when even the PSQRS system returns an access denial. If users do not obtain the desired results, they find other ways to reach their goal. Learning from the experience and the work of others will provide new and interesting adaptive solutions.

Acknowledgments. This work has been supported by the EUREKA project LINDO (ITEA2 – 06011).

References

1. Biskup, J.: Security in Computing Systems: Challenges, Approaches and Solutions, 1st edn. Springer Publishing Company, Incorporated (2008)
2. Harrison, M.A., Ruzzo, W.L., Ullman, J.D.: Protection in operating systems. Commun. ACM 19(8), 461–471 (1976)
3. N.I. of Standards and Technology, Assessment of access control systems, Interagency Report 7316 (2006)
4. Ferraiolo, D., Kuhn, D.: Role-based access controls. In: 15th National Computer Security Conference. NSA/NIST, pp. 554–563 (1992)
5. OASIS, A brief introduction to XACML (March 2003)
6. Bertino, E., Bonatti, P.A., Ferrari, E.: TRBAC: A temporal role-based access control model. ACM Trans. Inf. Syst. Secur. 4(3), 191–233 (2001)
7. Hansen, F., Oleshchuk, V.: SRBAC: A spatial role-based access control model for mobile systems. In: Proceedings of the 7th Nordic Workshop on Secure IT Systems (2003)
8. Zhang, G., Parashar, M.: Dynamic context-aware access control for grid applications. In: Proceedings of the 4th International Workshop on Grid Computing, pp. 101–108. IEEE Computer Society (2003)
9. Chae, S.H., Kim, W., Kim, D.-K.: uT-RBAC: Ubiquitous role-based access control model. IEICE Transactions 89-A(1), 238–239 (2006)
10. Kulkarni, D., Tripathi, A.: Context-aware role-based access control in pervasive computing systems. In: 13th ACM Symposium on Access Control Models and Technologies, SACMAT, pp. 113–122. ACM (2008)
11. Povey, D.: Optimistic security: a new access control paradigm. In: Proceedings of the 1999 Workshop on New Security Paradigms, pp. 40–45. ACM (1999)
12. Rissanen, E., Firozabadi, B.S., Sergot, M.J.: Towards a mechanism for discretionary overriding of access control. In: Christianson, B., Crispo, B., Malcolm, J.A., Roe, M. (eds.) Security Protocols 2004. LNCS, vol. 3957, pp. 312–319. Springer, Heidelberg (2006)
13. Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC), Break-glass - an approach to granting emergency access to healthcare systems. White paper (2004)

14. Catarci, T., de Leoni, M., Marrella, A., Mecella, M., Salvatore, B., Vetere, G., Dustdar, S., Juszczyk, L., Manzoor, A., Truong, H.-L.: Pervasive software environments for supporting disaster responses. IEEE Internet Computing 12, 26–37 (2008)
15. Kawagoe, K., Kasai, K.: Situation, team and role based access control. Journal of Computer Science 7(5), 629–637 (2011)
16. Sánchez, M., López, G., Cánovas, Ó., Sánchez, J.A., Gómez-Skarmeta, A.F.: An access control system for multimedia content distribution. In: Atzeni, A.S., Lioy, A. (eds.) EuroPKI 2006. LNCS, vol. 4043, pp. 169–183. Springer, Heidelberg (2006)
17. El-Khoury, V.: A multi-level access control scheme for multimedia database. In: Proceedings of the 9th Workshop on Multimedia Metadata, WMM 2009 (2009)
18. Chen, S.-C., Shyu, M.-L., Zhao, N.: Smarxo: towards secured multimedia applications by adopting rbac, xml and object-relational database. In: Proceedings of the 12th Annual ACM International Conference on Multimedia, pp. 432–435. ACM (2004)
19. Thuraisingham, B., Lavee, G., Bertino, E., Fan, J., Khan, L.: Access control, confidentiality and privacy for video surveillance databases. In: Proceedings of the Eleventh ACM Symposium on Access Control Models and Technologies, pp. 1–10. ACM (2006)
20. Brut, M., Codreanu, D., Dumitrescu, S., Manzat, A.-M., Sedes, F.: A distributed architecture for flexible multimedia management and retrieval. In: Hameurlain, A., Liddle, S.W., Schewe, K.-D., Zhou, X. (eds.) DEXA 2011, Part II. LNCS, vol. 6861, pp. 249–263. Springer, Heidelberg (2011)
21. Al Kukhun, D., Sedes, F.: Adaptive solutions for access control within pervasive healthcare systems. In: Helal, S., Mitra, S., Wong, J., Chang, C.K., Mokhtari, M. (eds.) ICOST 2008. LNCS, vol. 5120, pp. 42–53. Springer, Heidelberg (2008)